Remarks

Claims 2, 3, 28-30, 32-36, and 44-46 are pending in the application, with claim 46 being the independent claim.

Based on the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 112

Claim 45 was rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. Applicant respectfully traverses this rejection.

Claim 45 recites, in part: "decrypted data generated by the encryption component is passed to the authentication component and aligned by the authentication component." In support of the rejection, the Office Action states that "the dependent claims cannot change [the independent claim] order," (Office Action, p. 3). Applicant submits that claim 45 does not require a change in order. FIG. 3 of the present application illustrates path 309, connecting authentication engine 308 to crypto alignment block 354. FIG. 3 also illustrates path 359, connecting crypto engine 358 to authentication alignment block 304. Thus, data can traverse path 309 according to claim 46, and traverse path 359 according to claim 45, without a change in order. Accordingly, Applicant submits that the rejection is traversed. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Rejections under 35 U.S.C. § 103

Kaplan, Larsen, Huynh, and Fumy

Claims 2, 3, 28-30, 33, 35, 36, and 44-46 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaplan, U.S. Patent No. 6,704,871 ("Kaplan"), in view of Larsen, U.S. Patent No. 7,068,791 ("Larsen"), Huynh, U.S. Patent No. 6,983,366 ("Huynh"), and Fumy, *Internet Security Protocols*, ("Fumy"). Applicant respectfully traverses this rejection.

The Office Action parses the independent claim and applies these four references to separate elements of the claim out of context of the claim as a whole. As will be described herein, when the references are combined, the combination is incapable of operating as recited in independent claim 46.

Claim 46 recites, in part:

> "performing authentication operations on a set of header data and the payload data for the first packet to generate an authentication code;
> ...
> combining remaining payload data for the first packet with the authentication code for the first packet;
> adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block having a predefined length;
> performing encryption operations on the first packet data block;
> ...
> wherein the authentication and encryption operations for the first packet are performed within the chip in a single pass."

The Office Action alleges that Kaplan discloses the elements of "*performing authentication operations on a set of header data and the payload data for the first packet to generate an authentication code; performing encryption operations on a set of data in the payload data for the first packet, wherein the encryption operations on*

the set of payload data for the first packet is performed in parallel with the authentication operations for the first packet" recited in independent claim 46. The Office Action acknowledges that Kaplan does not disclose "*combining the remaining payload data for the first packet with the authentication code for the first packet; adding padding to the combined remaining payload data and authentication code*" recited in independent claim 46. (Office Action, p. 6.) However, the Office Action alleges that Fumy discloses this element.

The combination of Kaplan and Fumy is incapable of operating in the manner recited in independent claim 46. Fumy states that "[i]n the case of a block cipher, padding is added to force the length of the plaintext to be a multiple of the block cipher's block length." (Fumy, p. 199.) Fumy does not disclose "*combining the* ***remaining payload data for the first packet*** *with the authentication code for the first packet*" after a first set of data in the payload data has already been encrypted. Fumy simply states that padding is added to the plaintext to be a multiple of the block cipher.

Furthermore, Kaplan cannot support *"combining the remaining payload data for the first packet with the authentication code for the first packet; adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block having a predefined length; performing encryption operations of the first packet data block*" as recited in independent claim 1.

Kaplan relates to a pre-padding architecture whereby padding is added prior to encryption or hashing operations, such that encryption or hashing operations occur only after adding padding. Figure 9 of Kaplan illustrates a pad insertion block

associated with the encrypt/decrypt block, and a pad insertion block associated with the hash block. Each pad insertion block is positioned prior to its associated processing block. Kaplan therefore discloses that pad insertion must occur prior to, not after, encryption operations or hash operations on a data block, such that Kaplan cannot add padding to a generated authentication code.

For example, Kaplan discloses "[g]enerating and appending Pad bytes to the end of a Plaintext packet prior to encryption." (Kaplan, 41:20-21). As to the hash block, Kaplan discloses that "[i]n the case of hash-encrypt, where the two components of the operation are done in parallel, if any padding is added to the crypto block according to the option selected, the same padding is added to the hash block." (Kaplan, 42:50-54). Kaplan further discloses that "[f]or the Hash operations, padding is automatically added... prior to computing the hash." (Kaplan, 39:38-42). Thus, in contrast to claim 46, Kaplan clearly discloses that during parallel operations, pad insertion occurs prior to processing and hash operations.

Furthermore, in Kaplan, the output from the hash function is fed into the crypto-context block and "is always read from the digest register of the appropriate crypto-context." (*See* FIG. 9, 38:61-62.) As shown in FIG. 9, a read of context storage goes to the output bus.

In order to add "*padding to the combined remaining payload data and authentication code for the first packet*" as suggested by the Examiner, the payload data and authentication code of the message would need to be provided to the input FIFO and padded, if necessary, by pad insertion block as illustrated in FIG. 9. As pointed out above, Kaplan does not provide any disclosure or mechanism for feeding

the result of hash block into the input FIFO of encrypt block. Therefore, to operate as suggested by the Examiner, the authentication code must be calculated prior to providing the message to the input FIFO.

Thus, the combination of Kaplan and Fumy necessarily precludes "*performing authentication operations on a set of header data and the payload data for the first packet to generate an authentication code; performing encryption operations on a set of data in the payload data for the first packet, wherein the encryption operations on the set of payload data for the first packet is performed in parallel with the authentication operations for the first packet*" in addition to "*combining remaining payload data for the first packet with the authentication code for the first packet; adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block having a predefined length*" as recited in independent claim 46.

Larsen and Huynh fail to remedy the deficiencies of Kaplan and Fumy. For at least these reasons, independent claim 46 is patentable over the combination of Kaplan, Larsen, Huynh and Fumy. Claims 2, 3, 28-30, 33, 35, 36, 44, and 45 depend from independent claim 46. For at least the above reasons, and further in view of their own features, dependent claims 2, 3, 28-30, 33, 35, 36, 44, and 45 are patentable over the combination of Kaplan, Larsen, Huynh, and Fumy. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Kaplan, Larsen, Huynh, Fumy, and Ganapathy

Claim 32 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaplan, in view of Larsen, Huynh, and Fumy, and further in view of Ganapathy, U.S. Patent No. 6,557,096 ("Ganapathy"). Applicant respectfully traverses this rejection.

Claim 32 depends from independent claim 46. Ganapathy does not overcome the deficiencies of Kaplan, Larsen, Huynh, and Fumy described above relative to claim 46. For at least these reasons, and further in view of its own features, claim 32 is patentable over the combination of Kaplan, Larsen, Huynh, Fumy, and Ganapathy. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Kaplan, Larsen, Huynh, Fumy, and Gaytan

Claim 34 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaplan, in view of Larsen, Huynh, and Fumy, and further in view of Gaytan, U.S. Patent No. 5,638,367 ("Gaytan"). Applicant respectfully traverses this rejection.

Claim 34 depends from independent claim 46. Gaytan does not overcome the deficiencies of Kaplan, Larsen, Huynh, and Fumy described above relative to claim 46. For at least these reasons, and further in view of its own features, claim 34 is patentable over the combination of Kaplan, Larsen, Huynh, Fumy, and Gaytan. Reconsideration and withdrawal of the rejection is therefore respectfully requested.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicant
Registration No. 50,633

Date: October 15, 2009

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600